Using the Common Criteria in Smart Card Security

Gene Troy

National Institute of Standards & Technology

Gaithersburg, MD, USA

21 September 1999

Common Criteria General Model

What the Common Criteria is --

- Common structure & language for describing product/system IT security requirements (Part 1)
- Catalogs of standardized IT security requirement components & packages (Parts 2 & 3)

How the CC is used --

- Develop Protection Profiles and Security Targets -- specific IT security requirements for products & systems -- *Consumers then use them for decisions*
- Evaluate products & systems against known & understood requirements => CONFIDENCE

Protection Profiles

- **Protection Profile (PP):**
  An implementation-independent set of security objectives and requirements for a category of IT products or systems that meet similar consumer needs for IT security.
  - ***Examples: Firewall PP, C2-PP, CS2-PP, RBAC-PP***

The CC Evaluation Scheme

- Evaluation of IT security products under the CC is done within an “Evaluation Scheme” (agreed approach) by accredited laboratories.
- Laboratory evaluation work is done under the oversight of an “Evaluation Authority”
- The Evaluation Authority issues a certificate upon successful completion of an evaluation
- In the U.S., the Authority & operator of the Scheme is called “NIAP” - National Information Assurance Partnership (NIST & NSA)
- NIAP is a partner in the international Mutual Recognition Arrangement (MRA)

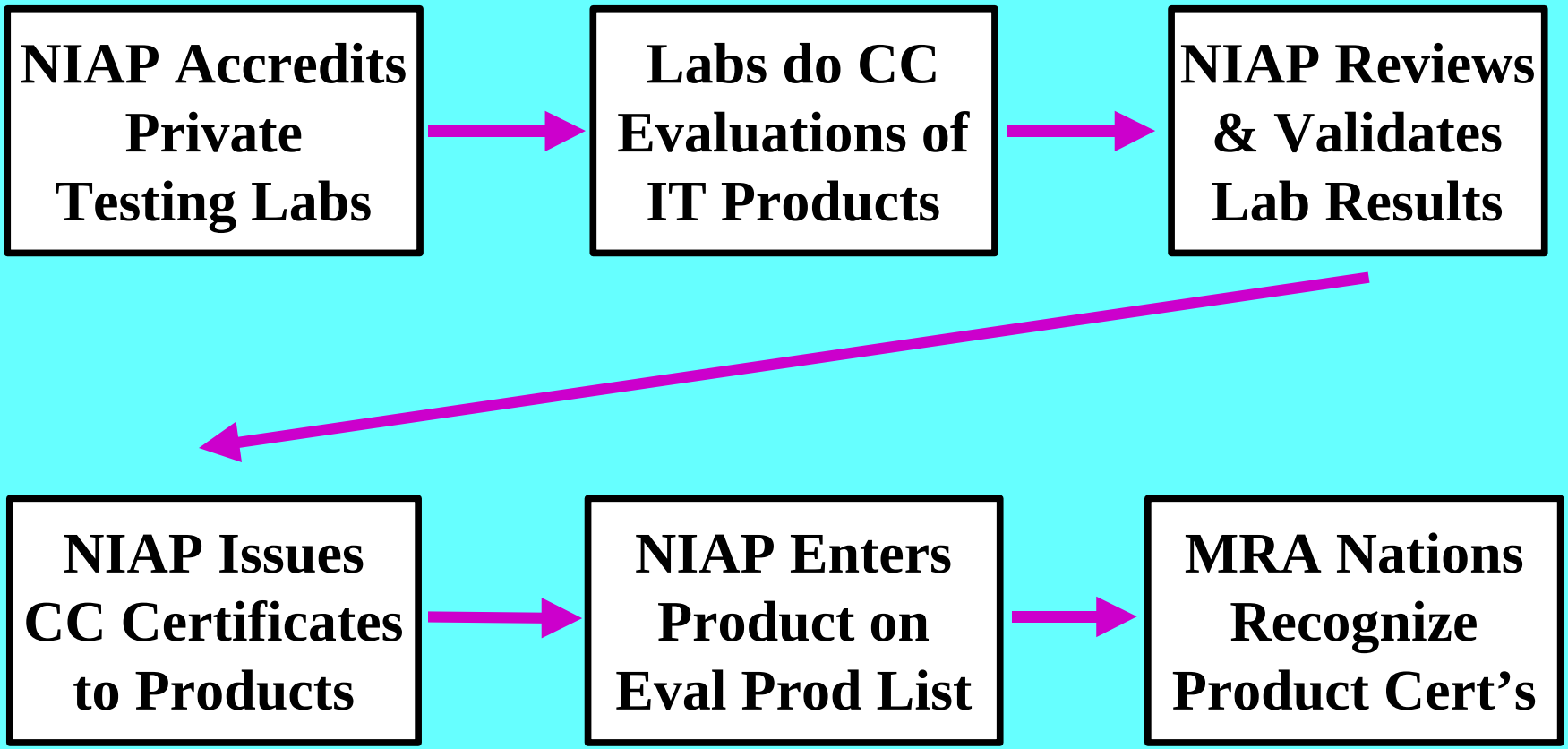
Mutual Recognition of Product Evaluations

Common Criteria Mutual Recognition Arrangement --

- Seven nations now members: Australia, Canada, France, Germany, New Zealand, United Kingdom, United States
- IT security evaluations conducted by US testing laboratories recognized by the other nations
- Eliminates duplicate, costly security evaluations for product developers
- More nations to be added in near future

- [Get the MRA at: http://niap.nist.gov/ccmra-v1.pdf]

US Evaluation Scheme -- Overview



Applying the CC to Smart Cards

- **Smart Card similarities to other IT products:**
  - **Mostly IT elements**
  - **Perform many IT functions (operating system, multiple applications, etc.)**
- **Smart Card differences from other IT products:**
  - **Unitary product (hardware-software-crypto-card)**
  - **Development process more complex**
  - **Trusted product in untrusted hands**
  - **Penetration risk greater**
  - **Security evaluation approach different**

A CC Application Opportunity

- NIAP was approached by Visa International to help develop:
  - Smart Card security requirements from issuer/user perspective
  - Product evaluation process taking Smart Card differences into account
- NIAP organized international credit card companies (financial payment systems) to work together to develop common requirements
- Smart Card Security Users Group (SCSUG) was born - 6/99

SCSUG - Mission Statement

Utilizing the infrastructure provided by the Common Criteria (ISO 15408) and the National Certification Schemes' Mutual Recognition Arrangement:

Develop and promote the use of standardized security requirements to ensure that the device security and data protection needs of the smart card end users are appropriately represented and met in the smart card products implemented by them.

Smart Card Security Users Group Members

- American Express
- Europay
- JCB
- Master Card
- Mondex
- Visa
- NIAP:
  - NIST
  - NSA
- Observers: CC Management Committee reps

SCSUG Task 1
Develop SCSUG PP

- Visa draft PP used as starting point
- Public review comments on Visa PP used as basis for new SCSUG PP
- Pre-release draft PP to Smart Card Vendors
- Public review draft on 1 November (to be posted on CC website -- http://csrc.nist.gov/cc)
- 90-day public comment period
- Finalized & evaluated by June 2000
- Evaluated final PP -- used by SCSUG Members

SCSUG Task 2
Lab Accreditation Criteria

- **Purpose: provide SCSUG Members' smart card lab selection experience to CC-MRA Organizations to aid their process of *accrediting qualified labs* to do CC-based evaluations**

SCSUG Task 3
Test Methods & Tests

- **Purpose: provide SCSUG Members' smart card lab testing experience to CC-MRA Organizations to aid their process of *developing smart card specific tests & methods* for use in CC-based evaluations**

SCSUG-Vendor Meeting

- Date: 21 September, 1999
- Location: NIST
- Attendees:
  - SCSUG Members
  - 19 Major Smart Card-related Vendors
- Purpose: Introduce Key Vendors to SCSUG & initiate dialog on developing common smart card security requirements
- Next Step: possibly organize Smart Card vendors to interact with expanding user community

Obtaining the SCSUG User-Oriented Smart Card PP

- PP Release date: 1 November 1999
- CC Website: http://csrc.nist.gov/cc

- Comment Period: 3 months
  - Start: 1 November 1999
  - End: 31 January 2000

- Format & Recipient for comments:
  (see posted instructions)